Commissaire
du Centre
de la sécurité
des télécommunications

Rapport annuel

2007-2008

Canada

Bureau du commissaire du Centre
de la sécurité des télécommunications
C.P. 1984, Succursale « B »
Ottawa (Ontario)
K1P 5R5

Tél. : (613) 992-3044
Téléc. : (613) 992-4096
Site Web : www.ocsec-bccst.gc.ca

© Ministre des Travaux publics et des
Services gouvernementaux Canada 2008
ISBN 978-0-662-05700-0
N° de cat. D95-2008

Photos de la couverture : Malak

FSC
Sources Mixtes
Groupe de produits issu de forêts bien gérées et d'autres sources contrôlées
Cert no. SW-COC-000789
www.fsc.org
© 1996 Forest Stewardship Council

Commissaire du Centre de la
sécurité des télécommunications

L'honorable Charles D. Gonthier, C.C., c.r.

Communications Security
Establishment Commissioner

The Honourable Charles D. Gonthier, C.C., Q.C.

Mai 2008

Ministre de la Défense nationale
Édifice MGen G.R. Pearkes, 13e étage
101, promenade Colonel-By, tour nord
Ottawa (Ontario)
K1A 0K2

Monsieur le ministre,

Conformément au paragraphe 273.63(3) de la *Loi sur la défense nationale*, j'ai le plaisir de vous communiquer mon rapport annuel de 2007–2008 sur mes activités et constatations, aux fins de présentation au Parlement.

Je vous prie d'agréer, monsieur le ministre, l'assurance de ma haute considération.

Charles D. Gonthier

P.O. Box/C.P. 1984, Station "B"/Succursale « B »
Ottawa, Canada
K1P 5R5
(613) 992-3044 Téléc. : (613) 992-4096

Ce rapport est dédié à la mémoire du

Très honorable Antonio Lamer
c.p., C.C., c.d., L.L.D., d.u.

1933–2007

TABLE DES MATIÈRES

Introduction /1

Le contexte d'examen /2
- Recommandations du Sous-comité de la Chambre des communes et du Comité sénatorial spécial sur la *Loi antiterroriste* /2
- Modifications proposées à la *Loi sur la défense nationale* /3
- L'enquête interne Iacobucci et la Commission d'enquête Major /6

Rétrospective de l'année /7
- Plan de travail /7
- Examens relatifs aux activités du CSTC /8
- Méthodologie /10
- Aperçu des constatations pour 2007–2008 /11

Points saillants de l'examen de 2007–2008 /13
- Examen des activités de collecte de renseignements électromagnétiques menées par le CSTC sous le régime d'une autorisation ministérielle (deuxième partie) /13
- Examen des activités liées à la sécurité des technologies de l'information au sein d'un ministère /14
- Examen des activités du CSTC exercées en vertu d'une directive ministérielle /15
- Examen des activités antiterroristes du CSTC /17
- Examen de l'assistance du CSTC au SCRS /18
- Examens en cours ou projetés /19
- Plaintes relatives aux activités du CSTC /20
- Fonctions exercées en vertu de la *Loi sur la protection de l'information* /20

Le bureau du commissaire /20

Hommage /22

Annexe A : Mandat du commissaire du Centre de la sécurité des télécommunications /23

Annexe B : Rapports classifiés au ministre, 1996–2008 /25

Annexe C : État des dépenses, 2007–2008 /29

Annexe D : Historique du Bureau du commissaire du Centre de la sécurité des télécommunications (BCCST) /31

Annexe E : Rôle et mandat du Centre de la sécurité des télécommunications Canada (CSTC) /33

INTRODUCTION

Ce rapport annuel est le deuxième que je publie à titre de commissaire du Centre de la sécurité des télécommunications et il paraît au milieu de mon mandat de trois ans.

Je veille à ce que soient respectés non seulement la lettre mais aussi l'esprit de la loi.

Une réflexion s'impose alors que j'ai franchi la moitié de mon premier mandat. Tout comme mes prédécesseurs, je veille à ce que soient respectés non seulement la lettre mais aussi l'esprit de la loi. Dans cette optique, je me penche sur des situations qui pourraient donner lieu à des activités non conformes à la loi et je formule mes recommandations de manière à écarter cette possibilité. Si j'estime qu'une telle activité peut avoir eu lieu, je dois bien entendu en informer le ministre de la Défense nationale et le procureur général du Canada.

Ceci m'amène à réfléchir sur une de mes préoccupations personnelles — le rôle de l'individu face aux comportements qu'il convient d'adopter. Pour exercer leurs fonctions, les employés du Centre de la sécurité des télécommunications Canada (CSTC)[1] ne doivent pas seulement posséder des compétences techniques. Il leur faut également avoir un respect fondamental pour la primauté du droit et la démocratie, ce qui englobe une attente raisonnable en matière de protection de la vie privée de tous les Canadiens. La culture organisationnelle du CSTC doit refléter ces valeurs, et le Centre doit élaborer et mettre en œuvre des politiques et des procédures qui découlent de la loi et témoignent de ces valeurs.

Il est très clair dans mon esprit que, depuis les attentats de 2001 et les activités terroristes qui ont suivi, le niveau de risque et la perception d'une menace ont augmenté pour de nombreux Canadiens, et il est peu probable que cela diminue. Cette situation impose à des gens comme les employés du CSTC un fardeau supplémentaire, car le gouvernement s'attend à ce qu'ils dépassent les aspects purement mécaniques de la collecte du renseignement. Ils sont appelés à saisir des renseignements qui serviront de fondement à des décisions judicieuses afin de protéger les Canadiens, mais de manière à protéger la vie privée.

[1] L'organisme porte le nom de Centre de la sécurité des télécommunications Canada depuis le 27 septembre 2007, conformément au Programme de coordination de l'image de marque du gouvernement du Canada.

Durant l'année écoulée, j'ai pu formuler certaines critiques à l'endroit de pratiques du CSTC qui, à mon avis, auraient avantage à être renforcées. J'estime toutefois que le fait saillant des derniers mois a été la manière dont le chef du CSTC a traité une question opérationnelle découverte à la fin de 2006 et qui posait un risque de non-conformité avec la loi. Le chef m'a informé de la situation sur-le-champ et il m'a ensuite tenu régulièrement au courant de toutes les mesures correctives prises. Par sa réaction mesurée, la direction du Centre a répondu aux besoins de l'organisation et a su montrer du respect pour les personnes qui en assurent le fonctionnement, tout en ne laissant planer aucun doute quant à leurs obligations.

LE CONTEXTE D'EXAMEN

Recommandations du Sous-comité de la Chambre des communes et du Comité sénatorial spécial sur la *Loi antiterroriste*

Dans le rapport final qu'il a présenté à la Chambre des communes le 27 mars 2007, le Sous-comité de la Chambre des communes chargé d'examiner la *Loi antiterroriste* omnibus a formulé un certain nombre de recommandations concernant le CSTC et mon bureau, notamment sur les ambiguïtés juridiques des dispositions relatives aux autorisations ministérielles. Depuis que la *Loi antiterroriste* a reçu la sanction royale en décembre 2001, mes prédécesseurs et moi-même sommes aux prises avec un dilemme persistant qui découle des changements que cette loi a apportés à la *Loi sur la défense nationale*. Un sujet particulièrement préoccupant est la divergence de vues entre mon bureau et le CSTC concernant les avis juridiques qui lui sont prodigués par le ministère de la Justice visant l'interprétation des dispositions relatives aux autorisations ministérielles.

Dans son rapport final, le Sous-comité encourageait l'avocat du gouvernement et moi-même à régler ce différend. De plus, il demandait que, dans sa réponse au Rapport final, le gouvernement précise, dans la mesure du possible, quels étaient les points de désaccord et comment ils avaient été résolus et que, à défaut, je fournisse ces détails dans mon rapport annuel de 2007–2008.

Le gouvernement a publié sa réponse le 18 juillet 2007, dans lequel il indique que « le CST collabore avec les fonctionnaires du ministère de la Justice afin de [...] régler [ces questions] et de faire adopter les modifications législatives proposées en temps opportun »[2]. Un an plus tard, il semble y avoir eu peu de progrès. En attendant que les choses évoluent, j'acquiesce à la demande du Sous-comité et j'explique deux de mes principales recommandations concernant les autorisations ministérielles.

Le gouvernement a indiqué que des modifications législatives seraient adoptées en temps opportun. Un an plus tard, il semble y avoir eu peu de progrès.

Modifications proposées à la *Loi sur la défense nationale*

La disposition relative aux autorisations ministérielles accordées aux seules fins de l'obtention du renseignement étranger est la suivante :

Autorisation ministérielle

273.65 (1) Le ministre peut, dans le seul but d'obtenir des renseignements étrangers, autoriser par écrit le Centre de la sécurité des télécommunications à intercepter des communications privées liées à une activité ou une catégorie d'activités qu'il mentionne expressément.

Conditions d'autorisation

(2) Le ministre ne peut donner une autorisation que s'il est convaincu que les conditions suivantes sont réunies :

a) l'interception vise des entités étrangères situées à l'extérieur du Canada;

b) les renseignements à obtenir ne peuvent raisonnablement être obtenus d'une autre manière;

[2] *Réponse du gouvernement du Canada au Rapport final du Sous-comité sur la revue de la* Loi antiterroriste, du *Comité permanent de la Chambre des communes sur la sécurité publique et nationale*, p. 22.

c) la valeur des renseignements étrangers que l'on espère obtenir grâce à l'interception justifie l'interception envisagée;

d) il existe des mesures satisfaisantes pour protéger la vie privée des Canadiens et pour faire en sorte que les communications privées ne seront utilisées ou conservées que si elles sont essentielles aux affaires internationales, à la défense ou à la sécurité.

[...]

Ma première recommandation principale concerne l'expression *activité ou catégorie d'activités* relativement au CSTC et au commissaire. Mes prédécesseurs et moi-même estimons depuis longtemps qu'une simple lecture de la *Loi* soutient l'interprétation selon laquelle l'interception autorisée par le ministre est celle d'une communication privée liée à une *activité ou une catégorie d'activités* qui est ciblée ou fait l'objet d'une enquête, et qu'elle ne constitue pas une méthode de collecte comme l'affirme le CSTC. Par conséquent, une modification importante serait de clarifier la signification de l'expression *activité ou catégorie d'activités*.

Ma seconde recommandation principale est de définir les termes *intercepter* et *interception*, ou d'établir un renvoi à la définition du terme *intercepter* qui se trouve dans le *Code criminel*. À l'heure actuelle, ces termes ne sont pas définis dans la *Loi sur la défense nationale*. Or, ils ont tous les deux une signification juridique et opérationnelle pour le CSTC.

En l'absence de définitions qui soient comprises et appliquées uniformément, il m'est difficile d'interpréter les pouvoirs conférés au CSTC et d'examiner la façon dont ils ont été appliqués.

Le Comité sénatorial spécial sur la *Loi antiterroriste* a aussi formulé des recommandations relatives aux autorisations ministérielles. Il a notamment recommandé « [q]ue les paragraphes 273.65(2) et (4) de la *Loi sur la défense nationale* soient modifiés de manière à préciser que les faits et opinions qui sont nécessaires afin de convaincre le ministre de la Défense nationale que toutes les conditions justifiant une autorisation écrite de recourir à l'interception des communications privées sont réunies, doivent être fondés sur une croyance raisonnable ou des soupçons raisonnables »[3].

[3] Comité sénatorial spécial sur la *Loi antiterroriste*, *Justice fondamentale dans des temps exceptionnels : Rapport principal du Comité sénatorial spécial sur la* Loi antiterroriste, février 2007, recommandation nº 18, p. 85.

La clarification dans la *Loi* de la norme à appliquer demeure une question à l'ordre du jour pour mon bureau, et je continue d'appuyer un tel amendement à la *Loi sur la défense nationale*.

Par ailleurs, j'ai recommandé aux représentants du CSTC et du ministère de la Justice d'autres modifications que je juge pertinentes.

En réponse à une autre recommandation du Sous-comité de la Chambre des communes, le gouvernement a fait savoir qu'il n'a pas l'intention de modifier la *Loi* afin de préciser que mon bureau devrait procéder à des examens des activités liées à l'interception pour déterminer si elles sont conformes à la *Charte canadienne des droits et libertés* et à la *Loi sur la protection des renseignements personnels*. Comme je l'ai signalé dans mon rapport annuel de l'an dernier, la méthode d'examen de mon bureau a toujours intégré une vérification de la conformité par rapport à toutes les lois pertinentes, y compris la *Charte* et la *Loi sur la protection des renseignements personnels*.

Le Sous-comité recommandait également dans son rapport final que le gouvernement établisse par voie législative un comité de parlementaires qui serait chargé d'examiner les questions de sécurité nationale et que ce comité soumette la *Loi antiterroriste* à un autre examen exhaustif à l'issue d'une période déterminée. Le gouvernement a répondu qu'il n'a pas décidé si telle était la meilleure façon de procéder. Il a toutefois indiqué qu'il « proposera une approche visant la sécurité nationale qui remplira les objectifs de base énoncés dans le deuxième rapport de la Commission d'enquête sur les actions des responsables canadiens relativement à Maher Arar; il étudie aussi des options pour accroître le rôle des parlementaires en tant qu'élément clé des propositions visant à mettre en place un meilleur cadre d'examen des mesures de sécurité nationale »[4]. Comme je l'ai indiqué dans mon rapport de l'an dernier, je suis d'accord avec mon prédécesseur qui a dit appuyer « l'idée d'un examen parlementaire plus dynamique des activités liées à la sécurité nationale », mais en soulignant « les défis qui y sont associés, notamment en ce qui a trait à la composition du comité et à son accès à des documents et renseignements classifiés »[5].

[4] *Supra*, note 2, p. 28.
[5] Commissaire du Centre de la sécurité des télécommunications, *Rapport annuel 2006–2007*, p. 8.

L'enquête interne Iacobucci et la Commission d'enquête Major

L'honorable Frank Iacobucci a entamé une enquête interne concernant les agissements des responsables canadiens relativement à Abdullah Almalki, Ahmad Abou-Elmaati et Muayyed Nureddin. Il doit déterminer, entre autres choses, si la détention ou tout mauvais traitement de ces personnes en Syrie ou en Égypte découle, directement ou indirectement, des actions de responsables canadiens, particulièrement en ce qui concerne l'échange de renseignements avec des pays étrangers et, le cas échéant, si ces actions comportaient des lacunes dans les circonstances.

L'honorable John Major fait enquête sur les mesures d'investigation prises à la suite de l'attentat à la bombe contre le vol 182 d'Air India. Il doit notamment établir si des changements de pratique ou législatifs s'imposent pour éviter d'autres problèmes similaires de coopération entre le Service canadien du renseignement de sécurité (SCRS) et la Gendarmerie royale du Canada (GRC), dans le cadre des enquêtes relatives à des infractions de terrorisme. Il doit également recommander au gouvernement des moyens d'établir une relation fiable et fonctionnelle entre les organismes du renseignement de sécurité et les organismes d'exécution de la loi relativement à l'utilisation du renseignement comme élément de preuve dans un procès criminel.

Je m'intéresse à l'échange de données concernant les Canadiens, particulièrement lorsque ces renseignements doivent être échangés à l'extérieur du Canada. C'est une question que mon bureau continue d'examiner. À cet égard, les conclusions des commissions Iacobucci et Major pourraient avoir une incidence sur les organismes du renseignement et de la sécurité, ainsi que sur les organismes d'examen, y compris mon bureau.

RÉTROSPECTIVE DE L'ANNÉE

L'an dernier, j'ai mentionné l'examen indépendant portant sur la gestion de mon bureau et les recommandations visant à améliorer nos méthodes. Après une étude approfondie, nous avons adopté des changements dans nos nouvelles politiques et procédures opérationnelles, et mon bureau les applique dans le cadre des examens. Un des plus notables est une nouvelle méthode qui porte sur l'examen des processus communs à plusieurs activités du CSTC. Elle devrait rendre la fonction d'examen plus efficace, au moins sur deux plans : en premier lieu, en évitant certaines répétitions; et en second lieu, en favorisant une compréhension plus complète et plus directe des activités au cœur du mandat du Centre. Celui-ci a été tenu au courant tout au long de la mise en œuvre de ces changements, et des questions précises de méthodologie ayant une incidence directe sur le Centre et sur nos relations de travail ont été discutées.

À ma demande, le CSTC a présenté plusieurs breffages à mon équipe. Certains sont devenus des événements annuels, comme les séances ayant trait à l'élaboration et à la mise à jour des politiques ou à la mise en œuvre d'un nouveau système de gestion de l'information. D'autres portaient sur les cybermenaces et certains aspects de la coopération avec le SCRS. À notre demande et conformément aux pratiques en vigueur, le CSTC nous a aussi donné des séances d'information au début de la plupart des examens entamés durant l'année.

Plan de travail

Un plan de travail triennal guide les activités de mon bureau. Ce plan, qui est revu régulièrement, fait partie intégrante du processus d'examen et constitue un pivot de la relation entre mon bureau et le CSTC. Chacune de ses mises à jour comporte une réévaluation de l'ordre de priorité des projets d'examen prévus ou possibles et prend en compte les nouveaux renseignements dont nous avons connaissance. Ainsi, un examen qui vient de se terminer peut faire ressortir un aspect qui dépasse la portée de l'examen même mais que j'estime utile d'approfondir, par exemple pour évaluer la conformité avec la loi ou assurer la protection de la vie privée des Canadiens. Dans mon rapport de l'an dernier, j'ai fait état d'autres

critères qui influent sur le choix des sujets inscrits au plan de travail. Cependant, je dois toujours évaluer l'importance relative des différentes questions pouvant faire l'objet d'un examen et être convaincu, dans la mesure du possible, que celles qui présentent les plus grands risques sur le plan du respect de la loi ou de la protection de la vie privée sont soumises à un examen.

Le CSTC est invité à donner son avis sur le plan de travail, et ce, pour plusieurs raisons : il est pratique courante de faire en sorte qu'aucun secteur de l'organisation ne soit soumis à une charge d'examen excessive; il doit y avoir un équilibre entre mon mandat d'examen et les obligations opérationnelles imposées au Centre par le gouvernement. En outre, il est important de voir à ce que l'échelonnement et la portée des projets d'examen soient raisonnables et à ce que ces projets soient réalisables dans des délais opportuns, compte tenu des ressources et des mandats des deux organismes.

Le CSTC et mon bureau ont pris l'initiative importante de tenir une table ronde sur nos relations de travail. L'objectif visé était d'optimiser le processus d'examen, afin notamment d'atténuer tout effet négatif sur les activités du Centre. La rencontre a permis de passer en revue les processus administratifs de part et d'autre, de s'entendre sur des points à améliorer et de proposer des moyens à cet effet. Des mesures ont été prises à la suite de questions soulevées au sujet du plan de travail. De l'avis général, ce genre de réunion a été utile et a contribué aux objectifs des deux organismes de maintenir des voies de communication ouvertes et de faire en sorte que les travaux d'examen donnent les résultats escomptés.

Examens relatifs aux activités du CSTC

Mon mandat général d'examen est énoncé à l'alinéa 273.63(2)*a)* de la *Loi sur la défense nationale*[6]. En vertu du paragraphe 273.65(8) de la *Loi*, je suis en outre tenu de vérifier si les activités découlant d'une autorisation ministérielle sont autorisées et d'en rendre compte au ministre.

[6] Se reporter à l'annexe A pour le libellé des articles pertinents de la *Loi sur la défense nationale*.

Les autorisations ministérielles pour la collecte de renseignements étrangers sont accordées en vertu du paragraphe 273.65(1) de la *Loi*, tandis que celles relatives à la sécurité des technologies de l'information le sont aux termes du paragraphe 273.65(3) de la *Loi*. J'entame mes examens des activités du CSTC découlant d'autorisations ministérielles après l'expiration de l'autorisation ministérielle.

Comme je l'ai mentionné dans mon dernier rapport annuel, « [c]ompte tenu des caractéristiques des technologies de communication modernes, le CST court le risque inhérent, lorsqu'il tente d'intercepter les communications d'entités qui se trouvent à l'étranger, d'intercepter en même temps des communications privées de Canadiens. C'est pourquoi il doit obtenir une autorisation ministérielle à cette fin »[7].

Les dispositions de l'autorisation ministérielle ne permettent pas au CSTC de cibler les communications de Canadiens. Cependant, en vertu de la *Loi sur la défense nationale*, le ministre peut, « dans le seul but d'obtenir des renseignements étrangers »[8], autoriser le Centre à intercepter des communications privées de Canadiens et de personnes au Canada dans la mesure où l'interception vise une entité étrangère située à l'extérieur du Canada. Les autorisations ministérielles relatives à la sécurité des technologies de l'information permettent aussi l'interception incidente de communications privées que le Centre peut capter alors qu'il assure la protection des systèmes et réseaux d'un ministère ou organisme fédéral.

De plus, lorsqu'il recueille des renseignements étrangers, le CSTC peut incidemment acquérir des renseignements personnels sur des Canadiens. Il peut conserver ces renseignements uniquement s'il les juge indispensables à la compréhension du renseignement étranger et peut les inclure dans ses rapports sur le renseignement étranger pour autant qu'ils soient supprimés (c'est-à-dire remplacés par une référence générique telle que « un Canadien »). Quand, par la suite, des ministères ou organismes fédéraux demandent au CSTC de divulguer des renseignements supprimés, le Centre exige qu'ils justifient leur droit de recueillir ces renseignements en

[7] *Supra*, note 5, p. 18.
[8] Paragraphe 273.65(1) de la *Loi sur la défense nationale*.

vertu de leurs mandats respectifs et qu'ils fournissent une justification opérationnelle de leur besoin de connaître cette information. Si ces conditions sont réunies, le Centre peut divulguer les renseignements supprimés. Cette année, deux de mes rapports comportaient des examens détaillés de ce genre de divulgation.

Durant l'exercice 2007–2008, mon bureau a remis au ministre cinq rapports classifiés basés sur des examens complétés au courant de l'année. Deux examens visaient des activités du CSTC menées en vertu d'une autorisation ministérielle, dont l'une portait sur la collecte de renseignements étrangers, et l'autre sur la sécurité des technologies de l'information. Les trois autres examens ont été réalisés en vertu de mon mandat général, soit d'évaluer si les activités du CSTC sont conformes à la loi et dans quelle mesure l'organisme protège la vie privée des Canadiens dans l'exécution de ses activités.

Méthodologie

Avant de commencer un examen, mon bureau fournit au CSTC un cadre de référence dans lequel sont énoncés l'objectif, la portée et les critères de l'examen, et qui renferme un résumé de l'approche à adopter et un calendrier d'exécution. Durant un examen, les examinateurs du BCCST emploient des outils et des techniques standard de recherche des faits pour recueillir des éléments de preuve, ce qui comprend l'examen de tous les documents imprimés et électroniques pertinents ainsi que des autorisations, politiques et procédures connexes. Les examinateurs effectuent aussi de nombreux essais ainsi que des prises d'échantillons. Ils procèdent à des entrevues avec les gestionnaires et les autres intervenants qui ont participé aux activités à l'étude. Ils peuvent également interroger des représentants d'autres ministères et organismes fédéraux. En outre, les opinions et avis juridiques sont examinés. Le CSTC donne des séances d'information et des démonstrations d'activités, et répond à des questions écrites. Au terme du processus, les examinateurs rencontrent les représentants du Centre pour passer en revue les constatations et conclusions de l'examen avant de mettre la dernière main à leur rapport.

Aperçu des constatations pour 2007-2008

Même si les cinq examens de l'année portaient sur des sujets différents, on note des thèmes récurrents, dont certains sont décrits ci-dessous. Dans l'ensemble, je peux constater que les activités du CSTC examinées au cours de l'année étaient conformes à la loi.

Interprétation des autorisations ministérielles

Comme je l'ai mentionné, le CSTC et mon bureau ne s'entendent toujours pas quant à l'interprétation des dispositions de la *Loi sur la défense nationale* relatives aux autorisations ministérielles. Cependant, d'ici l'adoption d'amendements législatifs, j'ai repris la pratique de mon prédécesseur, qui consiste à examiner si les activités du CSTC exécutées en vertu d'une autorisation ministérielle cadrent avec la *Loi* telle qu'elle a été interprétée par le ministère de la Justice, et à en rendre compte. Dans cette optique, je peux constater que les deux examens menés sur des activités découlant d'une autorisation ministérielle étaient conformes à la loi telle qu'elle est interprétée par le ministère de la Justice.

Gestion de l'information

Un thème qui revient régulièrement concerne des lacunes dans la gestion des documents et de l'information. Si l'information est correctement gérée, tous les renseignements et documents pertinents figurent dans les dossiers de l'organisation. Or, comme mes prédécesseurs et moi-même l'avons indiqué dans les rapports antérieurs, des renseignements inadéquats ou manquants dans les dossiers du CSTC peuvent entraver ma capacité d'effectuer des examens et d'établir si l'organisme a agi en conformité avec la loi. Par conséquent, il s'ensuit, là où je l'indique, que je ne puisse offrir au ministre que l'assurance négative que je n'ai aucune preuve de non-respect de la loi, à défaut d'une assurance positive qui s'appuierait sur une preuve de légalité. Le CSTC est tout à fait au courant de mes préoccupations à cet égard, il est résolu à trouver des solutions et il est en voie de mettre en œuvre un système de gestion des dossiers. Il me tient au courant de ses mesures en ce sens. À l'avenir, nos examens continueront à chercher des

Des renseignements inadéquats peuvent entraver ma capacité d'effectuer des examens.

documents qui démontrent une conformité aux instruments habilitants, qui consignent toutes les activités effectuées et qui prouvent que les superviseurs font un suivi du rendement de leur personnel.

Interprétation du mandat en matière de renseignement étranger

Dans le *Rapport annuel* de l'an dernier, j'ai indiqué qu'une des questions soulevées par mon examen de la collecte de renseignements étrangers par le CSTC à l'appui de la Gendarmerie royale du Canada était « de savoir si les demandes de renseignements de la GRC dans le cadre de ses enquêtes criminelles au pays relèvent [dans tous les cas du volet du mandat du CSTC concernant le renseignement étranger] »[9]. En attendant que les questions juridiques soulevées soient réexaminées, j'ai décidé qu'aucune évaluation ne serait faite de la légalité des activités d'assistance à la GRC, menées par le CSTC en vertu du volet de son mandat concernant le renseignement étranger, tel qu'il est interprété et appliqué en ce moment. Cette question n'était toujours pas réglée au 31 mars 2008. Mon examen de l'assistance que le CSTC prête au Service canadien du renseignement de sécurité, dont il est question ci-après, soulève des questions similaires. Comme je l'indique en l'occurrence, et contrairement à la question des autorisations ministérielles, je suis d'accord avec le conseil que le ministère de la Justice a fourni au CSTC. Toutefois, dans certains cas, je questionne en vertu de quel volet de son mandat le CSTC peut s'acquitter de ces activités. Mon équipe continue d'approfondir la question avec le CSTC.

[9] *Supra*, note 5, p. 13.

POINTS SAILLANTS DE L'EXAMEN DE 2007-2008

Examen des activités de collecte de renseignements électromagnétiques menées par le CSTC sous le régime d'une autorisation ministérielle (deuxième partie)

Contexte

Ce rapport porte sur le second et dernier volet d'un examen de certaines activités de collecte de renseignements étrangers exécutées en vertu de trois autorisations ministérielles qui étaient en vigueur de mars 2004 à décembre 2006. La première partie, dont j'ai rendu compte dans le dernier *Rapport annuel*, a permis de comprendre cette activité du Centre. Elle a aussi servi à examiner les pouvoirs, les politiques, les procédures et le cadre de gestion mis en place pour surveiller les activités, et à établir les critères d'examen de la deuxième partie.

L'objectif de la deuxième partie était d'évaluer et de vérifier si les activités effectuées aux termes des autorisations ministérielles respectaient la loi de même que les attentes énoncées dans une directive ministérielle connexe.

Conclusions

En ce qui concerne les conditions imposées par les autorisations ministérielles, prescrites au paragraphe 273.65(2) de la *Loi sur la défense nationale*, et les conditions imposées par le ministre dans le cadre du processus d'autorisation, je n'ai relevé aucune preuve de non-conformité avec la loi. Cependant, faute d'information et de documentation, mon bureau n'a pas pu vérifier la conformité à un certain nombre de conditions. L'examen a aussi permis de constater que, dans certains cas, le CSTC n'avait pas respecté les attentes établies dans la directive ministérielle, et j'en ai informé le ministre.

Nous avons constaté qu'il existe des politiques opérationnelles pour orienter le CSTC quant à la protection de la vie privée des Canadiens. Je n'ai trouvé aucune information portant à croire que le personnel du Centre contrevient aux politiques opérationnelles. Cependant, les données aux dossiers étant parfois absentes ou incomplètes, je ne peux fournir au ministre qu'une assurance négative, ce qui revient à dire que je n'ai trouvé aucune preuve de non-respect de la loi.

Examen des activités liées à la sécurité des technologies de l'information au sein d'un ministère

Contexte

Cet examen portait sur les activités liées à la sécurité des technologies de l'information menées par le CSTC au sein d'un ministère fédéral en vertu d'une autorisation ministérielle en 2004–2005. L'objectif était d'évaluer le respect de la loi ainsi que des dispositions de l'autorisation ministérielle.

Le CSTC est tenu, aux termes de la *Loi sur la défense nationale*, d'aider à protéger les systèmes et réseaux informatiques du gouvernement du Canada en analysant la vulnérabilité de certains systèmes informatiques et de télécommunication et en fournissant aux ministères et organismes gouvernementaux des conseils et des services touchant la sécurité des technologies de l'information.

Les activités du CSTC liées à la sécurité des technologies de l'information peuvent donner lieu à l'interception incidente de communications privées de Canadiens ou de renseignements personnels concernant un Canadien. Pour cette raison, voici ce qui est prévu au paragraphe 273.65(3) de la *Loi* :

> Le ministre peut, dans le seul but de protéger les systèmes ou les réseaux informatiques du gouvernement du Canada de tout méfait ou de toute utilisation non autorisée ou de toute perturbation de leur fonctionnement, autoriser par écrit le Centre de la sécurité des télécommunications à intercepter, dans les cas visés à l'alinéa 184(2)*c)* du *Code criminel*, des communications privées qui sont liées à une activité ou une catégorie d'activités qu'il mentionne expressément.

Le chef du CSTC est tenu d'obtenir, pour le compte du ministère ou de l'organisme, l'autorisation visant l'activité demandée. Cette autorisation permet au CSTC de procéder à une évaluation complète de la sécurité des réseaux du ministère.

Conclusions

L'examen a révélé que les activités du CSTC visant la sécurité des technologies de l'information dans le ministère étaient conformes à la loi et à l'autorisation ministérielle. Le processus d'obtention de l'autorisation ministérielle auquel a eu recours le CSTC respectait les dispositions de la *Loi sur la défense nationale* ainsi que les politiques connexes du Centre. Il a également été établi que les cinq conditions énoncées au paragraphe 273.65(4) de la *Loi* ont été respectées de manière satisfaisante. Des mesures étaient en place afin de protéger la vie privée des Canadiens, et l'utilisation et la conservation par le CSTC de renseignements personnels concernant des Canadiens étaient conformes à la loi et aux politiques de l'organisme.

Examen des activités du CSTC exercées en vertu d'une directive ministérielle

Contexte

Cet examen portait sur certaines activités entreprises par le CSTC en vertu d'une directive ministérielle et, dans le contexte d'autorisations ministérielles, à l'appui de son mandat de renseignement étranger énoncé à l'alinéa 273.64(1)*a)* de la *Loi sur la défense nationale*, pour la période du 1er avril 2005 au 31 mars 2006.

La complexité des technologies et des réseaux de télécommunications ne cesse de s'accroître. Pour accomplir le mandat que lui confère la loi, le CSTC cherche à comprendre l'infrastructure mondiale de l'information et à localiser les renseignements étrangers, conformément aux priorités du gouvernement du Canada en matière de renseignement.

L'examen avait pour objectif d'aider mon bureau à mieux comprendre ces activités et les autorisations sous-jacentes. Il a permis d'évaluer le respect des directives ministérielles et des lois du Canada par le CSTC, y compris la *Loi sur la défense nationale*, la *Charte* et la *Loi sur la protection des renseignements personnels* qui régit la collecte, l'utilisation et la divulgation de renseignements personnels. L'examen a aussi servi à évaluer dans quelle mesure les activités étaient conformes aux politiques et aux procédures du CSTC.

Conclusions

C'était la première fois que mon bureau examinait ces activités mises en œuvre sous le régime d'une directive ministérielle. Je suis convaincu que le CSTC prend des mesures afin de protéger la vie privée des Canadiens lorsqu'il utilise et conserve les données découlant de ces activités. J'ai néanmoins formulé un certain nombre de recommandations présentées ci-après.

En premier lieu, j'estime que le CSTC devrait réexaminer sa pratique selon laquelle seules les communications privées reconnues par certains membres du personnel doivent faire l'objet d'un rapport. J'ai recommandé que d'autres employés qui observent et traitent des communications privées soient également tenus de rendre compte de ces communications. En second lieu, le CSTC devrait réévaluer de quel volet de son pouvoir législatif devrait relever certaines de ces activités, en particulier celles concernant des renseignements fournis par des organismes fédéraux chargés de l'application de la loi et de la sécurité. Enfin, je suis d'avis que le Centre devrait renforcer ses politiques et procédures afin de mieux orienter et soutenir ces activités.

Les employés qui observent et traitent des communications privées devraient être tenus d'en rendre compte.

Mon bureau a appris depuis lors que le CSTC réexamine ces activités ainsi que les politiques et procédures connexes. Je soutiens cette initiative, et j'entends maintenir un suivi des points soulevés durant cet examen.

Examen des activités antiterroristes du CSTC

Contexte

Cet examen a porté sur la légalité des activités antiterroristes du CSTC au cours de la période du 1er avril au 31 juillet 2005.

Au début d'octobre 2001, le CSTC a centralisé les efforts déployés dans le domaine du renseignement étranger relativement aux menaces provenant du terrorisme international, et a procédé à la recherche et à l'analyse de données du renseignement étranger afin d'identifier les cibles terroristes et leurs réseaux d'opération et de soutien. Ces données peuvent être échangées avec les ministères et organismes fédéraux chargés du renseignement et de la sécurité, de même qu'avec les principaux partenaires du Canada en matière de renseignement.

L'objectif principal était d'examiner la collecte de données et les rapports préparés pendant la période d'examen pour vérifier que les renseignements ont été recueillis, utilisés et conservés de manière conforme à la loi, et pour relever et signaler toute autre source de préoccupation pouvant avoir une incidence sur l'aptitude du CSTC à mener à bien ses activités en toute légalité et à protéger la vie privée des Canadiens.

Conclusions

Cet examen a permis de conclure que les activités exécutées étaient conformes à la loi ainsi qu'aux politiques du CSTC. Les membres du personnel interrogés étaient bien informés des instruments qui régissent leur travail. Le rapport renferme deux recommandations visant à renforcer la responsabilité du CSTC : d'une part, relativement aux liens entre les rapports préparés par le Centre et les priorités du gouvernement du Canada en matière de renseignement; d'autre part, relativement à l'utilisation et à la conservation des communications et des renseignements privés concernant des Canadiens.

Examen de l'assistance du CSTC au SCRS

Contexte

Cet examen portait sur la légalité des activités du CSTC lorsqu'il fournit une assistance au Service canadien du renseignement de sécurité (SCRS) en vertu du mandat en matière de renseignement étranger dévolu au CSTC, au cours de la période du 1er avril 2004 au 31 mars 2005, et comportait l'examen d'échantillons prélevés pour la période comprise entre novembre et décembre 2006.

Le CSTC transmet régulièrement des comptes rendus sur le renseignement étranger au SCRS. La plupart de ces rapports signalent des points d'intérêt général qui complètent et soutiennent les responsabilités qui incombent au SCRS. Le CSTC reçoit aussi certaines demandes d'information du SCRS liées au renseignement, et il y donne suite dans la mesure où elles cadrent avec les priorités du gouvernement du Canada en la matière. Un dernier aspect de l'assistance que le Centre prête au SCRS porte sur la divulgation de l'identité de Canadiens qui a été supprimée des rapports sur le renseignement étranger. Lorsqu'il reçoit une demande officielle à cet effet, le Centre doit déterminer que la justification est satisfaisante et être convaincu du droit légitime du demandeur.

Conclusions

Dans l'ensemble, je suis d'avis que le CSTC a respecté son mandat lorsqu'il a prêté assistance au SCRS. Je suis d'accord avec les conseils que le ministère de la Justice a offerts au Centre à ce sujet. Cependant, je questionne en vertu de quel volet de son mandat le CSTC peut s'acquitter de ces activités dans certains cas et j'ai recommandé au CSTC de réexaminer la question. Au 31 mars 2008, les pourparlers se poursuivaient entre mes représentants et le CSTC.

En outre, mon bureau a relevé des sources de préoccupation en ce qui concerne les demandes de divulgation de renseignements supprimés et le protocole d'entente de 1990 qui guide la collaboration entre le SCRS et le CSTC. Nombre de mes conclusions renforcent celles de deux examens antérieurs qui portaient sur la collecte de renseignements étrangers par le CSTC à l'appui de la GRC et sur les rôles exercés par les agents des relations avec la clientèle et la Section des politiques

opérationnelles du Centre relativement à la divulgation de renseignements personnels. Ces examens sont présentés dans mon rapport annuel de 2006–2007.

Je suis heureux de constater que, depuis la fin de la période d'examen, le Centre poursuit l'étude de ses processus, politiques et procédures internes dans l'intention d'apporter des améliorations là où des lacunes ont été signalées.

Le CSTC continue d'apporter des améliorations là où des lacunes ont été signalées.

J'ai cependant recommandé que le CSTC révise le protocole d'entente conclu avec le SCRS, qui n'est plus à jour et ne rend plus compte des arrangements ou pratiques actuels entre les deux organismes. Dans un contexte de menaces à l'échelle internationale, je suis d'avis que la coopération entre les organismes de sécurité et ceux du renseignement doit faire l'objet d'un examen continu et que les structures de collaboration doivent être revues périodiquement.

Examens en cours ou projetés

Mon bureau a entamé plusieurs examens dont je rendrai compte au ministre au cours de la prochaine année et dont je ferai état dans mon prochain rapport annuel. Entre autres sujets d'examen, mentionnons les activités effectuées par le CSTC en vertu de plusieurs autorisations ministérielles de collecte de renseignements étrangers; la divulgation de renseignements concernant des Canadiens à des ministères et organismes fédéraux; certaines pratiques du CSTC communes aux activités prévues par son mandat; et une étude exhaustive de ses activités liés à la sécurité des technologies de l'information. Certains examens engagés au cours du prochain exercice se poursuivront jusqu'en 2009–2010. L'an dernier, j'ai indiqué que je rendrais compte de l'usage par le CSTC de technologies pour protéger la vie privée des Canadiens. Au terme de l'exercice financier, cet examen était en voie d'être complété, et sera donc présenté dans le rapport annuel de l'an prochain.

Plaintes relatives aux activités du CSTC

Dans le cadre de mon mandat, je dois procéder à toute enquête que je considère nécessaire par suite d'une plainte. Durant l'année financière 2007–2008, mon bureau n'a reçu aucune plainte ayant nécessité une enquête officielle.

Fonctions exercées en vertu de la *Loi sur la protection de l'information*

La *Loi sur la protection de l'information* m'autorise à recevoir des renseignements de personnes astreintes au secret à perpétuité qui veulent se prévaloir de la défense « d'intérêt public » concernant la divulgation de renseignements classifiés relatifs au CSTC. Aucun problème de ce genre n'a été soumis à mon bureau en 2007–2008.

LE BUREAU DU COMMISSAIRE

Je suis toujours secondé par un effectif de huit employés à temps plein et par un certain nombre d'experts contractuels auxquels nous faisons appel au besoin.

Un défi constant pour mon bureau est de rester au fait des technologies pour appuyer l'examen des activités du CSTC. Cette tâche a été simplifiée cette année par le Centre lui-même. À l'automne 2007, le Centre a ouvert ses portes aux membres de mon équipe qui ont suivi deux cours destinés à son personnel : un cours sur la sécurité des technologies de l'information et un autre sur le renseignement étranger.

En mai 2007, lors d'une réunion qui s'est tenue à Ottawa, j'ai entretenu les membres du Conseil consultatif sur la sécurité nationale, organisme créé en avril 2004 dans le cadre de la Politique de sécurité nationale. Formé de personnes extérieures au gouvernement, le Conseil a pour rôle de formuler des conseils sur des questions de sécurité.

En mai également, mon bureau a été l'hôte de la Tribune des organismes d'examen, qui a réuni les membres du Comité de surveillance des activités de renseignement de sécurité, du Bureau de l'Inspecteur général du Service canadien du renseignement de sécurité, de la Commission des plaintes du public contre la Gendarmerie royale du Canada et de mon propre bureau. La Tribune donne aux analystes chargés des examens l'occasion de comparer différentes pratiques optimales et de discuter de questions d'intérêt mutuel. À cet égard, la méthodologie d'examen de mon bureau a été discutée longuement.

En juin 2007, j'ai eu le plaisir de présenter le juge Antonin Scalia de la Cour suprême des États-Unis au Colloque international sur l'administration de la justice et la sécurité nationale dans les pays démocratiques, qui a eu lieu à Ottawa. Parrainé conjointement par la Cour fédérale du Canada et le Canadian Centre of Intelligence and Security Studies de l'Université Carleton, ce colloque m'a permis de renouer avec des collègues d'autres pays dont j'avais rencontrés certains en octobre 2006 à la dernière Conférence internationale des organismes de surveillance du renseignement (IIRAC), en Afrique du Sud.

En juin toujours, la directrice exécutive de mon bureau m'a représenté à une conférence internationale sur la responsabilité des organismes du renseignement et de la sécurité et des droits de la personne, tenue à La Haye sous les auspices du comité néerlandais de surveillance des services du renseignement et de la sécurité et de la Faculté de droit de l'Université Radboud de Nimègue. En septembre, le directeur des Opérations m'a représenté à la conférence annuelle de l'Association canadienne pour les études de renseignement et de sécurité, à Calgary, où les participants ont examiné les nombreux défis qui se posent dans les milieux du renseignement et de la sécurité.

En septembre, j'ai pris part à une conférence de deux jours intitulée « Protecting Security and Human Rights: The Case for Migration in Canada » et parrainée par l'Institut de recherche en politiques publiques.

Toutes ces initiatives témoignent d'un intérêt grandissant, au Canada et à l'étranger, pour les questions de sécurité et du renseignement et leurs nombreuses dimensions.

Depuis sa création en 1996 par décret en vertu de la partie II de la *Loi sur les enquêtes*, le Bureau du commissaire du CST est financé par le ministère de la Défense nationale, mais il a reçu de l'aide et un soutien administratif du Bureau du Conseil privé.

À l'automne, il a été décidé de mettre fin à la relation de longue date entre le BCCST et le Bureau du Conseil privé et de confier au ministère de la Défense nationale les fonctions de soutien administratif et autre de mon bureau. Ce changement me semble positif. Je m'en voudrais cependant de ne pas souligner l'aide et l'appui exceptionnels que nous avons reçus de l'équipe du Bureau du Conseil privé au cours des douze dernières années. Un grand merci de la part de nous tous.

On peut trouver de l'information sur le BCCST en consultant le site Web (www.ocsec-bccst.gc.ca), qui explique notre mandat et nos activités. Au cours de l'année financière 2007–2008, le site a reçu plus de 98 000 visites provenant notamment d'une quarantaine de pays à l'extérieur de l'Amérique du Nord.

En 2007–2008, les dépenses de mon bureau se sont chiffrées à 1 220 999 $ et ont été largement couvertes par le budget approuvé pour cette période. On trouvera un résumé de ces dépenses à l'annexe C.

HOMMAGE

Le 24 novembre 2007, le très honorable Antonio Lamer, mon prédécesseur à titre de commissaire du CST, est décédé à l'âge de 74 ans. Avocat et juriste de renom, il avait été nommé à la Cour suprême du Canada en 1980, avant de devenir juge en chef en 1990, poste qu'il a occupé jusqu'à sa retraite en 2000.

Antonio Lamer a été mon collègue à la Cour pendant plus de 11 ans et mon ami de longue date. Il lègue à la jurisprudence canadienne une contribution exceptionnelle, que seul surpasse son profond attachement au Canada. Il laisse un grand vide.

ANNEXE A : MANDAT DU COMMISSAIRE DU CENTRE DE LA SÉCURITÉ DES TÉLÉCOMMUNICATIONS

***Loi sur la défense nationale* – partie V.1**

273.63 (1) Le gouverneur en conseil peut nommer, à titre inamovible pour une période maximale de cinq ans, un juge à la retraite surnuméraire d'une juridiction supérieure qu'il charge de remplir les fonctions de commissaire du Centre de la sécurité des télécommunications.

(2) Le commissaire a pour mandat

a) de procéder à des examens concernant les activités du Centre pour en contrôler la légalité;

b) de faire les enquêtes qu'il estime nécessaires à la suite de plaintes qui lui sont présentées;

c) d'informer le ministre et le procureur général du Canada de tous les cas où, à son avis, le Centre pourrait ne pas avoir agi en conformité avec la loi.

(3) Le commissaire adresse au ministre, dans les quatre-vingt-dix jours suivant la fin de chaque exercice, un rapport sur l'exercice de ses activités. Le ministre dépose le rapport devant chacune des chambres du Parlement dans les quinze premiers jours de séance de celle-ci suivant sa réception.

(4) Dans l'exercice de son mandat, le commissaire a tous les pouvoirs conférés à un commissaire en vertu de la partie II de la *Loi sur les enquêtes*.

(5) Le commissaire peut retenir les services de conseillers juridiques ou techniques ou d'autres collaborateurs dont la compétence lui est utile dans l'exercice de ses fonctions; il peut fixer, avec l'approbation du Conseil du Trésor, leur rémunération et leurs frais.

(6) Le commissaire exerce les attributions que lui confèrent la présente partie et toute autre loi fédérale; il peut en outre se livrer à toute activité connexe autorisée par le gouverneur en conseil.

(7) La personne qui occupe, à l'entrée en vigueur du présent article, la charge de commissaire du Centre de la sécurité des télécommunications est maintenue en fonctions jusqu'à l'expiration de son mandat.

[...]

273.65 (8) Le commissaire du Centre de la sécurité des télécommunications est tenu de faire enquête sur les activités qui ont été exercées sous le régime d'une autorisation donnée en vertu du présent article pour en contrôler la conformité; il rend compte de ses enquêtes annuellement au ministre.

Loi sur la protection de l'information

15. (1) Nul ne peut être déclaré coupable d'une infraction prévue aux articles 13 ou 14 s'il établit qu'il a agi dans l'intérêt public. [...]

(5) Le juge ou le tribunal ne peut décider de la prépondérance des motifs d'intérêt public en faveur de la révélation que si la personne s'est conformée aux exigences suivantes : [...]

b) dans le cas où elle n'a pas reçu de réponse de l'administrateur général ou du sous-procureur général du Canada dans un délai raisonnable, elle a informé de la question, avec tous les renseignements à l'appui en sa possession : [...]

(ii) soit le commissaire du Centre de la sécurité des télécommunications si la question porte sur une infraction qui a été, est en train ou est sur le point d'être commise par un membre du Centre de la sécurité des télécommunications dans l'exercice effectif ou censé tel de ses fonctions pour le compte de celui-ci, et n'en a pas reçu de réponse dans un délai raisonnable.

ANNEXE B : RAPPORTS CLASSIFIÉS AU MINISTRE, 1996-2008

1. Principal vs. agent status – 3 mars 1997 (TRÈS SECRET)

2. Operational policies with lawfulness implications – 6 février 1998 (SECRET)

3. CSE's activities under *** – 5 mars 1998 (TRÈS SECRET Mot codé/ Réservé aux Canadiens)

4. Internal investigations and complaints – 10 mars 1998 (SECRET)

5. CSE's activities under *** – 10 décembre 1998 (TRÈS SECRET/Réservé aux Canadiens)

6. On controlling communications security (COMSEC) material – 6 mai 1999 (TRÈS SECRET)

7. How we test (Rapport classifié sur la mise à l'essai des pratiques du CST en matière de collecte et de conservation de renseignements électromagnétiques, et évaluation des efforts de l'organisme pour sauvegarder la vie privée des Canadiens) – 14 juin 1999 (TRÈS SECRET Mot codé/Réservé aux Canadiens)

8. A study of the *** collection program – 19 novembre 1999 (TRÈS SECRET Mot codé/Réservé aux Canadiens)

9. On *** – 8 décembre 1999 (TRÈS SECRET/COMINT)

10. A study of CSE's *** reporting process — an overview (Phase I) – 8 décembre 1999 (SECRET/Réservé aux Canadiens)

11. A study of selection and *** — an overview – 10 mai 2000 (TRÈS SECRET/ Réservé aux Canadiens)

12. CSE's operational support activities under *** — follow-up – 10 mai 2000 (TRÈS SECRET/Réservé aux Canadiens)

13. Internal investigations and complaints — follow-up – 10 mai 2000 (SECRET)

14. On findings of an external review of CSE's ITS program – 15 juin 2000 (SECRET)

15. CSE's policy system review – 13 septembre 2000 (TRÈS SECRET/ Réservé aux Canadiens)

16. A study of the *** reporting process — *** (Phase II) – 6 avril 2001 (SECRET/Réservé aux Canadiens)

17. A study of the *** reporting process — *** (Phase III) – 6 avril 2001 (SECRET/Réservé aux Canadiens)

18. CSE's participation *** – 20 août 2001 (TRÈS SECRET/Réservé aux Canadiens)

19. CSE's support to ***, as authorized by *** and code-named *** – 20 août 2001 (TRÈS SECRET/Réservé aux Canadiens)

20. A study of the formal agreements in place between CSE and various external parties in respect of CSE's Information Technology Security (ITS) – 21 août 2002 (SECRET)

21. CSE's support to ***, as authorized by *** and code-named *** – 13 novembre 2002 (TRÈS SECRET/Réservé aux Canadiens)

22. CSE's *** activities carried out under the *** 2002 *** Ministerial authorization – 27 novembre 2002 (TRÈS SECRET/Réservé aux Canadiens)

23. Lexicon of CSE definitions – 26 mars 2003 (TRÈS SECRET)

24. CSE's activities pursuant to *** Ministerial authorizations including *** – 20 mai 2003 (SECRET)

25. CSE's support to ***, as authorized by *** and code-named *** — Part I – 6 novembre 2003 (TRÈS SECRET/COMINT/Réservé aux Canadiens)

26. CSE's support to ***, as authorized by *** and code-named *** — Part II – 15 mars 2004 (TRÈS SECRET/COMINT/Réservé aux Canadiens)

27. A review of CSE's activities conducted under *** Ministerial authorization – 19 mars 2004 (SECRET/Réservé aux Canadiens)

28. Internal investigations and complaints — follow-up – 25 mars 2004 (TRÈS SECRET/Réservé aux Canadiens)

29. A review of CSE's activities conducted under 2002 *** Ministerial authorization – 19 avril 2004 (SECRET/Réservé aux Canadiens)

30. Review of CSE *** operations under Ministerial authorization – 1er juin 2004 (TRÈS SECRET/COMINT)

31. CSE's support to *** – 7 janvier 2005 (TRÈS SECRET/COMINT/ Réservé aux Canadiens)

32. External review of CSE's *** activities conducted under Ministerial authorization – 28 février 2005 (TRÈS SECRET/COMINT/Réservé aux Canadiens)

33. A study of the *** collection program – 15 mars 2005 (TRÈS SECRET/COMINT/ Réservé aux Canadiens)

34. Report on the activities of CSE's *** – 22 juin 2005 (TRÈS SECRET)

35. Interim report on CSE's *** operations conducted under Ministerial authorization – 2 mars 2006 (TRÈS SECRET/COMINT)

36. External review of CSE *** activities conducted under Ministerial authorization – 29 mars 2006 (TRÈS SECRET/Réservé aux Canadiens)

37. Review of CSE'S foreign intelligence collection in support of the RCMP (Phase II) – 16 juin 2006 (TRÈS SECRET/COMINT/Réservé aux Canadiens)

38. Review of information technology security activities at a government department under ministerial authorization – 18 décembre 2006 (TRÈS SECRET)

39. Review of CSE signals intelligence collection activities conducted under ministerial authorizations (Phase I) – 20 février 2007 (TRÈS SECRET/COMINT/ Réservé aux Canadiens)

40. Role of the CSE's client relations officers and the Operational Policy Section in the release of personal information – 31 mars 2007 (TRÈS SECRET/COMINT/ Réservé aux Canadiens)

41. Review of information technology security activities at a government department under ministerial authorization – 20 juillet 2007 (TRÈS SECRET)

42. Review of CSEC's counter-terrorism activities – 16 octobre 2007 (TRÈS SECRET/COMINT/Réservé aux Canadiens)

43. Review of CSE's activities carried out under a ministerial directive – 9 janvier 2008 (TRÈS SECRET/COMINT/Réservé aux Canadiens)

44. Review of CSEC's support to CSIS – 16 janvier 2008 (TRÈS SECRET/COMINT/Réservé aux Canadiens)

45. Review of CSEC signals intelligence collection activities conducted under ministerial authorizations (Phase II) – 28 mars 2008 (TRÈS SECRET/COMINT/Réservé aux Canadiens)

ANNEXE C : ÉTAT DES DÉPENSES, 2007-2008

Sommaire des articles courants

Traitements et salaires	713 135 $
Transports et télécommunications	37 431
Information	21 239
Services professionnels et spéciaux	257 488
Location	151 894
Achat de services de réparation et d'entretien	3 538
Fournitures et approvisionnements	8 652
Acquisition de machine et de matériel	23 258
Autres charges	4 364
Total	**1 220 999 $**

ANNEXE D : HISTORIQUE DU BUREAU DU COMMISSAIRE DU CENTRE DE LA SÉCURITÉ DES TÉLÉCOMMUNICATIONS (BCCST)

Le Bureau du commissaire du Centre de la sécurité des télécommunications (BCCST) a été créé le 19 juin 1996, au moment de la nomination du premier commissaire, l'honorable Claude Bisson, O.C., ancien juge en chef du Québec. M. Bisson a occupé le poste de commissaire jusqu'en juin 2003. Le très honorable Antonio Lamer, c.p., C.C., c.d., L.L.D., d.u., juge en chef du Canada (à la retraite), lui a alors succédé pour un mandat de trois ans. L'honorable Charles D. Gonthier, C.C., c.r., qui a pris sa retraite de la Cour suprême du Canada en 2003, a été nommé commissaire en août 2006.

Pendant les six premières années de son mandat (de juin 1996 à décembre 2001), le commissaire a exercé ses fonctions conformément à plusieurs décrets, pris en vertu de la partie II de la *Loi sur les enquêtes*. Au cours de cette période, il a assumé une double responsabilité : examiner les activités du Centre de la sécurité des télécommunications Canada (CSTC) afin de déterminer si elles étaient en conformité avec les lois du Canada, et recevoir les plaintes relatives aux activités du CSTC.

Dans le sillage des attentats terroristes du 11 septembre 2001, le Parlement a adopté la *Loi antiterroriste* omnibus, qui a été promulguée le 24 décembre 2001. Cette loi modifie la *Loi sur la défense nationale*, en y ajoutant la partie V.1, qui établit le cadre législatif du BCCST et du CSTC, et elle confie au commissaire de nouvelles responsabilités relatives à l'examen des activités que mène le CSTC sous le régime d'une autorisation ministérielle.

En outre, la *Loi* omnibus a remplacé la *Loi sur les secrets officiels* par la *Loi sur la protection de l'information*, laquelle attribue au commissaire des fonctions précises pour les cas où une personne astreinte au secret à perpétuité souhaiterait invoquer la défense de l'intérêt public pour justifier la divulgation de renseignements classifiés sur le CSTC.

En vertu de son mandat actuel, qui inscrit dans la loi le mandat initial établi en 1996 ainsi que les nouvelles responsabilités supplémentaires décrites ci-dessus, le commissaire conserve tous les pouvoirs que confère à un commissaire la partie II de la *Loi sur les enquêtes*.

ANNEXE E : RÔLE ET MANDAT DU CENTRE DE LA SÉCURITÉ DES TÉLÉCOMMUNICATIONS CANADA (CSTC)

Le Centre de la sécurité des télécommunications Canada (CSTC) est l'organisme national de cryptologie du Canada. Organisme unique en son genre au sein de la collectivité canadienne de la sécurité et du renseignement, le CSTC emploie des cryptologues pour protéger la sécurité des technologies de l'information du gouvernement du Canada et lui fournir des renseignements étrangers. Il offre en outre une assistance technique et opérationnelle aux organismes fédéraux chargés de la sécurité et de l'application de la loi.

Les produits et services de renseignement étranger du CSTC sont fournis à l'appui des décisions gouvernementales dans les domaines de la sécurité nationale, du renseignement national et de la politique étrangère. Ses activités en matière de renseignement électromagnétiques visent exclusivement des renseignements étrangers et sont assujetties aux priorités du gouvernement du Canada en matière de renseignement.

Dans le domaine de la sécurité des technologies de l'information, les produits et services du CSTC permettent à ses clients (les autres ministères et organismes gouvernementaux) d'assurer la sécurité de leurs systèmes et réseaux d'information électronique. Le CSTC effectue aussi des travaux de recherche-développement au nom du gouvernement du Canada dans des disciplines liées à la sécurité des télécommunications.

Le paragraphe 273.64(1) de la partie V.1 de la *Loi sur la défense nationale* établit le mandat du CSTC, qui comprend trois volets désignés sous le nom de parties a), b) et c) :

a) acquérir et utiliser l'information provenant de l'infrastructure mondiale d'information dans le but de fournir des renseignements étrangers, en conformité avec les priorités du gouvernement du Canada en matière de renseignement;

b) fournir des avis, des conseils et des services pour aider à protéger les renseignements électroniques et les infrastructures d'information importantes pour le gouvernement du Canada;

c) fournir une assistance technique et opérationnelle aux organismes fédéraux chargés de l'application de la loi et de la sécurité dans l'exercice des fonctions que la loi leur confère.

COMMUNICATIONS
SECURITY
ESTABLISHMENT
COMMISSIONER

Annual Report

2007-2008

Canada

Office of the Communications Security
Establishment Commissioner
P.O. Box 1984
Station "B"
Ottawa, Ontario
K1P 5R5

Tel.: (613) 992-3044
Fax: (613) 992-4096
Website: www.ocsec-bcest.gc.ca

© Minister of Public Works and
Government Services Canada 2008
ISBN 978-0-662-05700-0
Cat. No. D95-2008

Cover photos: Malak

Communications Security
Establishment Commissioner

The Honourable Charles D. Gonthier, C.C., Q.C.

Commissaire du Centre de la
sécurité des télécommunications

L'honorable Charles D. Gonthier, C.C., c.r.

May 2008

Minister of National Defence
MGen G.R. Pearkes Building, 13th Floor
101 Colonel By Drive, North Tower
Ottawa, Ontario
K1A 0K2

Dear Sir:

Pursuant to subsection 273.63(3) of the *National Defence Act*, I am pleased to submit to you my 2007–2008 annual report on my activities and findings, for your submission to Parliament.

Yours sincerely,

Charles Gonthier

Charles D. Gonthier

P.O. Box/C.P. 1984, Station "B"/Succursale «B»
Ottawa, Canada
K1P 5R5
(613) 992-3044 Fax: (613) 992-4096

This report is dedicated to the memory of

The Right Honourable Antonio Lamer
P.C., C.C., C.D., LL.D., D.U.

1933–2007

TABLE OF CONTENTS

Introduction /1

The Review Environment /2

- House of Commons Subcommittee and Special Senate Committee recommendations on the *Anti-terrorism Act* /2
- Proposed amendments to the *National Defence Act* /3
- Iacobucci Internal Inquiry and the Major Commission of Inquiry /6

The Year in Review /7

- Workplan /7
- Reviews undertaken of the activities of CSEC /9
- Methodology /10
- Overview of 2007–2008 findings /11

2007–2008 Review Highlights /13

- Review of CSEC signals intelligence collection activities conducted under ministerial authorizations (Phase II) /13
- Review of information technology security activities at a government department /14
- Review of CSEC's activities carried out under a ministerial directive /15
- Review of CSEC's counter-terrorism activities /17
- Review of CSEC's support to CSIS /18
- Reviews underway and planned /19
- Complaints about CSEC activities /20
- Duties under the *Security of Information Act* /20

The Commissioner's Office /20

A Tribute /22

Annex A: Mandate of the Communications Security Establishment Commissioner /23

Annex B: Classified Reports to the Minister, 1996–2008 /25

Annex C: Statement of Expenditures, 2007–2008 /29

Annex D: History of the Office of the Communications Security Establishment Commissioner (OCSEC) /31

Annex E: Role and Mandate of the Communications Security Establishment Canada (CSEC) /33

INTRODUCTION

This is my second annual report as Communications Security Establishment Commissioner, and its publication occurs at the mid-point in my three-year term.

The fact that I am halfway through my first mandate gives me pause for reflection. Like my predecessors, I seek assurance of compliance with the spirit of the law, and not just the letter. In this regard, I am concerned with situations where lack of compliance with the law may arise, and I tailor my recommendations to safeguard against that possibility. If I determine there may not have been compliance with the law, I must of course inform the Minister of National Defence and the Attorney General of Canada.

I seek assurance of compliance with the spirit of the law, and not just the letter.

This leads me to contemplate one of my personal preoccupations—the role of the individual in doing the right thing. In the case of the Communications Security Establishment Canada (CSEC),[1] the people who are doing the work must have more than just technical ability. They must also have a fundamental respect for the rule of law and for democracy, which includes a reasonable expectation of privacy for all Canadians. CSEC's organizational culture must reflect these values, and CSEC must develop and follow policies and procedures that flow from the law and the values.

It is very clear to me that as a result of the terrorist acts of 2001, as well as subsequent terrorist activities, many Canadians continue to live with a heightened sense and level of risk, and there is little likelihood that these will diminish. This places a greater burden on people such as those employed at CSEC, because the government relies upon them to go beyond the mechanical aspects of information collection. They are called upon to reach for information that will support good decision making and thereby protect Canadians, but in a way that safeguards privacy.

[1] The name was changed to Communications Security Establishment Canada effective September 27, 2007, in order to comply with the Government of Canada's Federal Identity Program.

During the past year, I may at times have been critical of certain of CSEC's practices that, in my opinion, could be strengthened. I hold the view, however, that the striking point of the last several months has been the CSEC Chief's handling of an operational issue that came to light at the end of 2006 that had the potential for non-compliance. The Chief informed me about the matter at once, and has kept me apprised on a regular basis of all corrective steps taken. CSEC management's measured response addressed the needs of the organization, and was at the same time respectful of the people who serve in it, while leaving no doubt as regards their obligations.

THE REVIEW ENVIRONMENT

House of Commons Subcommittee and Special Senate Committee recommendations on the *Anti-terrorism Act*

In its Final Report presented to the House of Commons on March 27, 2007, the Subcommittee of the House of Commons reviewing the omnibus *Anti-terrorism Act* made a number of recommendations concerning CSEC and my office, dealing particularly with the legal ambiguities in the provisions allowing for ministerial authorizations. Since the *Anti-terrorism Act* received Royal Assent in December 2001, my predecessors and I have faced a persistent dilemma arising from the amendments this Act introduced to the *National Defence Act*. Particularly troublesome has been the lack of agreement between my office and CSEC concerning the legal advice provided to CSEC by the Department of Justice. At issue is the interpretation given to the provisions relating to ministerial authorizations.

The Subcommittee's Final Report urged government counsel and me to resolve the issues concerning ministerial authorizations. As well, the Subcommittee requested that the Government's response to the Final Report indicate, to the extent possible, what the issues of disagreement are and how they have been resolved. Failing this, the Subcommittee encouraged me to provide these details in my 2007–2008 Annual Report.

The Government issued its response on July 18, 2007. It noted that "CSE is working with Department of Justice officials to address these issues, with a view to bringing forward proposed legislative amendments in due course."[2] One year later, there appears to have been a lack of progress. In the meantime, I wish to respond to the Subcommittee's request and to describe two of my principal recommendations relating to ministerial authorizations.

The Government noted that legislative amendments would be brought forward "in due course". One year later, there appears to have been a lack of progress.

Proposed amendments to the *National Defence Act*

The provision relating to ministerial authorizations issued for the sole purpose of obtaining foreign intelligence reads as follows:

Ministerial authorization

273.65 (1) The Minister may, for the sole purpose of obtaining foreign intelligence, authorize the Communications Security Establishment in writing to intercept private communications in relation to an activity or class of activities specified in the authorization.

Conditions for authorization

(2) The Minister may only issue an authorization under subsection (1) if satisfied that

(a) the interception will be directed at foreign entities located outside Canada;

(b) the information to be obtained could not reasonably be obtained by other means;

[2] *Response of the Government of Canada to the Final Report of the House of Commons Standing Committee on Public Safety and National Security Subcommittee on the review of the* Anti-terrorism Act, p. 20.

> *(c)* the expected foreign intelligence value of the information that would be derived from the interception justifies it; and
>
> *(d)* satisfactory measures are in place to protect the privacy of Canadians and to ensure that private communications will only be used or retained if they are essential to international affairs, defence or security.
>
> [...]

My first principal recommendation concerns the term *activity or class of activities* as it relates to CSEC and to the Commissioner. My predecessors and I have long held the view that a plain reading of the *National Defence Act* supports the interpretation that the interception authorized by the Minister is that of a private communication in relation to an *activity or class of activities* which is targeted or the object of inquiry, and not to a method of collection as contended by CSEC. Therefore, an important amendment would be to clarify the meaning of the term *activity or class of activities*.

My second principal recommendation is to define the terms *intercept* and *interception*, or to provide a reference to the existing definition of *intercept* in the *Criminal Code*. At present, these terms are not defined in the *National Defence Act*. However, they have both legal and operational significance for CSEC.

In the absence of definitions that are universally understood and consistently applied, it is difficult for me to interpret CSEC's legislated authority and to review how it has been applied.

The Special Senate Committee on the *Anti-terrorism Act* also made recommendations relating to ministerial authorizations. Notably, the Committee recommended "that subsections 273.65(2) and (4) of the *National Defence Act* be amended to clarify whether the facts and opinions, which are necessary to satisfy the Minister of National

Defence that all of the preconditions for issuing a written authorization to intercept private communications have been met, should be based on reasonable belief or reasonable suspicion".[3] Clarifying in law the standard to be used remains an issue of interest to my office, and I continue to support making such an amendment to the *National Defence Act*.

In addition, I have made other recommendations to officials at CSEC and at the Department of Justice for amendments that I think would be worthwhile to enact.

In response to another recommendation of the House of Commons' Subcommittee, the Government indicated that it did not intend to modify the *National Defence Act* to specify that my office should review interception activities for compliance with the *Canadian Charter of Rights and Freedoms* and the *Privacy Act*. As I pointed out in last year's Annual Report, my office's review methodology has always included an examination of compliance with all relevant laws, including the *Charter* and the *Privacy Act*.

The Subcommittee's Final Report also recommended that the Government proceed with legislation to establish a National Security Committee of Parliamentarians responsible for the review of national security matters, and that this Committee be called upon to conduct a further comprehensive review of the *Anti-terrorism Act* after a fixed period. The Government responded that it has not determined if this is the best way to proceed. However, it went on to note that it "will propose an approach to national security review that will meet the basic objectives set out in the second report of the Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar and is considering options for an enhanced role for Parliamentarians as a key

[3] Special Senate Committee on the *Anti-terrorism Act*, *Fundamental Justice in Extraordinary Times: Main Report of the Special Senate Committee on the* Anti-terrorism Act, February 2007, recommendation 18, p.78.

part of these proposals for an improved national security review framework."[4] As I commented in my report last year, I concur with my predecessor's position that welcomes "the prospect of more active parliamentary review of national security activities," while also noting "challenges such as the composition of the committee and its access to classified information and documents."[5]

Iacobucci Internal Inquiry and the Major Commission of Inquiry

The Honourable Frank Iacobucci is in the process of conducting an internal inquiry into the actions of Canadian officials in relation to Abdullah Almalki, Ahmad Abou-Elmaati and Muayyed Nureddin. He is to determine, amongst other matters, whether the detention or any mistreatment of these individuals in Syria or Egypt resulted, directly or indirectly, from actions of Canadian officials, particularly in relation to the sharing of information with foreign countries and, if so, whether those actions were deficient in the circumstances.

The Honourable John Major is conducting an inquiry into the investigation of the bombing of Air India Flight 182. In particular, he is to determine whether any changes in practice or legislation are required to prevent the recurrence of similar problems of cooperation between the Canadian Security Intelligence Service (CSIS) and the Royal Canadian Mounted Police (RCMP) in the investigation of terrorism offences, and to recommend how government should go about establishing a reliable and workable relationship between security intelligence and law enforcement agencies regarding the use of intelligence as evidence in a criminal trial.

I have an interest in the sharing of information about Canadians, particularly when that information is to be shared outside Canada. This is an area that my office continues to examine. In this context, the outcomes of the Iacobucci and Major Commissions may have an impact on security and intelligence agencies, as well as review agencies, including my office.

---

[4] *Supra*, note 2 at p. 25.

[5] Communications Security Establishment Commissioner, *Annual Report 2006–2007*, p. 8.

THE YEAR IN REVIEW

Last year, I referred to the independent management review of the operations of my office, and to recommendations to improve our methodology. These matters have been thoroughly examined, and changes have been incorporated in new operational policies and procedures. My office has been implementing these changes in the conduct of reviews. One of the most notable is a new approach that involves examining processes which are common to several different CSEC activities. As a result, the review function is expected to be more effective in at least two ways: first, by avoiding a certain amount of duplication; and second, by creating a greater and readier understanding of underlying activities at the core of CSEC's mandate. CSEC has been kept informed throughout the process of implementing these changes, and specific issues of methodology that have a direct impact on that organization and on our working relationship have been discussed.

At my request, CSEC provided several briefings to my staff during the past year. Some of the briefings have become annual occurrences, such as those related to policy developments and updates, and also to the implementation of a new information management system. Other briefings have dealt with cyber-threat activities and with certain aspects of cooperation with CSIS. As is standard practice, and at our request, CSEC also provided briefings at the beginning of most reviews initiated during the year.

Workplan

A three-year workplan guides the activities of my office. It is an integral component of the review process as well as being a focal point in the relationship between my office and CSEC. It is updated on a regular basis. Each update involves a re-assessment of the priority of planned and potential review projects and incorporates new information that may have come to our attention. For example, a review that has just been

completed may identify an area outside the scope of that review but which I believe needs to be examined further, perhaps to assess compliance with the law or to ensure the protection of the privacy of Canadians. In my report last year, I listed other criteria that contribute to determining what areas or topics will be included in the workplan. I must, however, always weigh what is reviewed against what is not, and be satisfied to the extent possible that those areas of greater risk to compliance with the law or to privacy are being examined.

CSEC is consulted on the workplan. There are several reasons for this. This is a standard practice in review to ensure that no one area of the organization is unduly burdened. There must be balance between my review mandate and CSEC's operational requirements mandated by the government. Another significant reason is that there is a need to ensure that the scheduling and scope of review projects is reasonable and can be carried out in a timely manner, taking into consideration the resources and mandates of both organizations.

An important initiative agreed upon by both CSEC and my office was to organize a roundtable discussion focussed on the working relationship. The objective was to optimize the review process, which as well means minimizing any adverse impact on the activities of CSEC. The meeting reviewed the business processes of both groups, identified points where improvement was desirable and proposed how to achieve those improvements. A number of issues related to the workplan were also identified and have been implemented. There was general agreement that this type of meeting was useful and served the interests of both organizations to keep open the lines of communication and to ensure that review works as intended.

Reviews undertaken of the activities of CSEC

My general review mandate is set out in paragraph 273.63(2)(a) of the *National Defence Act*.[6] Under subsection 273.65(8) of the Act, I also have an obligation to review and report to the Minister as to whether the activities carried out under a ministerial authorization are authorized.

Ministerial authorizations for foreign intelligence collection are issued under the authority of subsection 273.65(1) of the *National Defence Act*, whereas ministerial authorizations for information technology security activities are issued under subsection 273.65(3) of the Act. My reviews of CSEC's activities conducted under ministerial authorizations are undertaken after the ministerial authorization has expired.

As I noted in my Annual Report last year: "The characteristics of contemporary communications technology mean that the interception of communications by CSE, directed at foreign entities outside Canada, runs the inherent risk of acquiring the private communications of Canadians. It is for this reason that a ministerial authorization is sought for this collection."[7]

The ministerial authorization provisions do not allow CSEC to target Canadian communications. However, "for the sole purpose of obtaining foreign intelligence"[8], the Minister may authorize the interception of private communications of Canadians or persons in Canada as long as the interception was the result of CSEC's targeting a foreign entity located outside Canada. Ministerial authorizations for information technology security activities also authorize the interception of private communications that may be incidentally obtained by CSEC while protecting the systems and networks of a federal government department or agency.

---

[6] Please see Annex A for the text of the relevant sections of the *National Defence Act*.
[7] *Supra*, note 5 at p. 18.
[8] Subsection 273.65(1) of the *National Defence Act*.

Further, when collecting foreign intelligence, CSEC may also incidentally acquire information about Canadians. This information may only be retained if it is assessed as essential to the understanding of the foreign intelligence, and it may be included in foreign intelligence reporting if it is suppressed (i.e., replaced by a generic reference such as "a Canadian person"). When receiving a subsequent request for disclosure of the details of the suppressed information, CSEC requires federal government departments and agencies to explain their authority to collect this information under their own respective mandates and to provide an operational justification of their need to know this information. If these conditions are met, CSEC may release the suppressed information. This year, two of my reports included detailed reviews of such releases.

During 2007–2008, my office submitted to the Minister five classified reports based on reviews completed during the year. Two of the reviews dealt with CSEC's activities conducted under ministerial authorization; one of these pertained to foreign intelligence collection, while the other concerned information technology security. The other three reviews were conducted under my general mandate, to assess whether CSEC's activities were in compliance with the law, and the extent to which it protected the privacy of Canadians in carrying out the activities.

Methodology

Prior to beginning a review, my office provides CSEC with terms of reference that set out the objective, scope, criteria, a summary of the approach to be taken, and a timetable for the review. In conducting a review, OCSEC reviewers employ standard fact-finding tools and techniques to gather evidence, including examination of all relevant written and electronic records, and the associated authorities, policies and procedures. Reviewers also conduct extensive testing and sampling. Interviews are held with management and other personnel involved in the activities under review. Officials from other federal government departments and agencies may also be interviewed. In addition, legal

opinions and advice are examined. CSEC provides briefs and demonstrations of activities as well as answers to written questions. At the conclusion of the review process, reviewers meet with CSEC officials prior to finalizing their report. The purpose of this meeting is to outline review findings and conclusions.

Overview of 2007–2008 findings

Although the five reviews reported on this year differed in subject, there were recurring themes, some of which are noted below. Overall, I am able to report that the activities of CSEC examined during the year complied with the law.

Interpretation of ministerial authorizations

As noted earlier, CSEC and my office are still on opposite pages as regards the interpretation of the provisions of the *National Defence Act* relating to ministerial authorizations. However, pending legislative amendments, I have continued my predecessor's practice of reviewing and reporting on whether CSEC's activities conducted under ministerial authorization comply with the Act as it has been interpreted by the Department of Justice. On this basis, I am able to report that the two reviews of activities conducted under ministerial authorizations complied with the *National Defence Act* as interpreted by the Department of Justice.

Information management

The theme of weak document and information management has been a consistent one over time. Good information management ensures that all relevant information and documentation is entered into the corporate record. However, as I and my predecessors have noted in previous reports, inadequate or missing information in CSEC's corporate records can impair my ability to conduct reviews and to determine whether CSEC's activities comply with the law. This has left me, in some instances, in a position of providing only a negative assurance to the Minister that I have no

Inadequate information can impair my ability to conduct reviews.

evidence of non-compliance with the law, rather than providing positive assurance, supported by evidence of compliance. CSEC is well aware of my concerns in this regard, is committed to addressing this issue, and is making progress in implementing a corporate records management system. CSEC is keeping me informed of its efforts. Future reviews will continue to seek documentation that demonstrates compliance with authorities, provides a record of all activities conducted, and confirms that supervisors are monitoring the performance of their staff.

Interpretation of foreign intelligence mandate

In last year's Annual Report, I noted that one of the issues raised by my review of CSEC's foreign intelligence collection in support of the RCMP was "whether [the foreign intelligence part of CSEC's mandate] was the appropriate authority in all instances for CSE to provide intelligence support to the RCMP in the pursuit of its domestic criminal investigations."[9] Pending a re-examination of the legal issues raised, I decided that no assessment would be made of the lawfulness of CSEC's activities in support of the RCMP under the foreign intelligence part of CSEC's mandate as it is currently interpreted and applied. This issue remained unresolved as of March 31, 2008. My review of CSEC's support to CSIS, which is reported on below, raised similar issues. As I note in this instance, and unlike the matter of ministerial authorizations, I am in agreement with the advice that the Department of Justice has provided to CSEC. However, in certain cases, I question which part of CSEC's mandate should be used as the proper authority for conducting these activities. Discussions on these matters are ongoing.

[9] *Supra*, note 5 at p. 13.

Review of CSEC signals intelligence collection activities conducted under ministerial authorizations (Phase II)

Background

This report is the second and final phase of a review of certain foreign intelligence collection activities conducted under three ministerial authorizations that were in effect from March 2004 to December 2006. The first phase, which I reported on in last year's Annual Report, established an understanding of this foreign intelligence collection. It also examined the authorities, policies, procedures and management framework put in place to oversee the activities, and established the review criteria for this second phase.

The objective of this second phase was to assess and verify whether the activities that were authorized under the ministerial authorizations complied with the law as well as with the expectations set out in a ministerial directive relating to these activities.

Findings

With respect to the conditions imposed by the ministerial authorizations, which are articulated in subsection 273.65(2) of the *National Defence Act*, and the conditions imposed by the Minister as part of the authorization process, I found no evidence of non-compliance with the law. For a number of conditions, however, a lack of information and documentation did not allow my office to verify compliance. The review also found that, in some instances, CSEC had not complied with expectations set out in the ministerial directive, and I have so advised the Minister.

Operational policies were found to be in place and to provide direction to CSEC in the protection of the privacy of Canadians. No information was found to indicate that the actions of CSEC staff were in contravention of the operational policies. However, the absence and incompleteness of recorded information limits me to providing only a negative assurance to the Minister. That is to say that I have found no evidence of non-compliance with the law.

Review of information technology security activities at a government department

Background

This review examined information technology security activities conducted by CSEC under ministerial authorization in 2004–2005 at a government department. The objective was to assess compliance with the law and with the provisions of the ministerial authorization.

The *National Defence Act* mandates CSEC to help protect the Government of Canada's computer systems and networks by analyzing the vulnerability of selected computing and telecommunications systems and by providing information technology security advice and services to government departments and agencies.

CSEC's information technology security activities may result in the inadvertent interception of private communications of Canadians or personal information about a Canadian. For this reason, subsection 273.65(3) of the *National Defence Act* provides that:

> The Minister may, for the sole purpose of protecting the computer systems or networks of the Government of Canada from mischief, unauthorized use or interference, in the circumstances specified in paragraph 184(2)(c) of the *Criminal Code*, authorize the Communications Security Establishment in writing to intercept private communications in relation to an activity or class of activities specified in the authorization.

The CSEC Chief is responsible for seeking authorization on behalf of the department or agency requesting the activity to be covered. This ministerial authorization enables CSEC to undertake a complete security assessment of a department's networks.

Findings

The review found that CSEC's information technology security activities at the department were in compliance with the law and with the ministerial authorization. The process by which CSEC acquired the ministerial authorization was in accordance with the requirements of the *National Defence Act* and the processes outlined in CSEC's related policies. It was also determined that the five conditions set out in subsection 273.65(4) of the Act were complied with satisfactorily. Measures were in place to protect the privacy of Canadians, and CSEC's use and retention of personal information about Canadians was found to comply with the law and CSEC policy.

Review of CSEC's activities carried out under a ministerial directive

Background

This review focused on certain activities undertaken by CSEC under a ministerial directive and, in the context of ministerial authorizations, in support of its foreign intelligence mandate articulated in paragraph 273.64(1)(a) of the *National Defence Act* for the period of April 1, 2005 to March 31, 2006.

Technology and telecommunications networks continue to increase in complexity. In order to fulfill its legislative mandate, CSEC conducts activities for the purposes of understanding the global information infrastructure and of locating foreign intelligence, in accordance with the intelligence priorities of the Government of Canada.

The objective of this review was to increase my office's knowledge of these activities and the authorities under which the activities are conducted. The review assessed CSEC's compliance with the ministerial directive and with the laws of Canada, including the *National Defence Act*, the *Charter*, and the *Privacy Act*, which governs the collection, use and disclosure of personal information. The review also assessed whether the activities conformed to CSEC's policies and procedures.

Findings

This was my office's first examination of this activity, as governed by the ministerial directive. I am satisfied that CSEC takes measures to protect the privacy of Canadians in the use and retention of data obtained from this activity. However, I made a number of recommendations, as follows.

First, I believe that CSEC should re-examine its practice that only those private communications recognized by certain staff be accounted for. I recommended that other staff that observe and handle private communications should also be responsible for accounting for them. Second, CSEC should re-assess which part of its legislative authority ought to be used to conduct certain of these activities, particularly those involving information provided by federal law enforcement and security agencies. Finally, I also believe that CSEC should augment its policy and procedures in order to better guide and support these activities.

Staff that observe and handle private communications should be responsible for accounting for them.

My office has since been advised that CSEC is re-examining these activities and associated policies and procedures. I support CSEC's initiative, and will continue to monitor the issues raised during this review.

Review of CSEC's counter-terrorism activities

Background

This review examined the lawfulness of CSEC's counter-terrorism activities in the period from April 1 to July 31, 2005.

In early October 2001, CSEC centralized foreign intelligence efforts as they relate to threats from international terrorism. The activities involve research and analysis of foreign intelligence data in order to identify terrorist targets and their operational and support networks. The information may be shared with federal government departments and agencies involved in intelligence and security-related matters, as well as with Canada's principal intelligence partners.

The main objectives of the review were to examine data collection and reports from the review period to verify that the information was collected, used and retained in compliance with the law, and to identify and report on any other issue of concern that might impact on the ability of CSEC to conduct its activities lawfully and to safeguard the privacy of Canadians.

Findings

This review found that the activities conducted were in compliance with the law and with CSEC policy. Personnel who were interviewed during the course of this review were knowledgeable about the authorities governing their work. The report makes two recommendations. One would enhance accountability regarding linkages between CSEC reporting and the intelligence priorities of the Government of Canada, and the other would enhance accountability for the use and retention of private communications and information about Canadians.

Review of CSEC's support to CSIS

Background

The objective of this review was to assess the lawfulness of CSEC's activities in providing support to the Canadian Security Intelligence Service (CSIS) under CSEC's foreign intelligence mandate in the period from April 1, 2004 to March 31, 2005 and a sampling from November to December 2006.

CSEC provides regular foreign intelligence reporting to CSIS. Most of this reporting addresses general areas of interest that complement and support CSIS' own mandated responsibilities. CSEC also receives and responds to specific CSIS requests for intelligence-related information, provided that the requirement is consistent with documented Government of Canada intelligence priorities. A final aspect of CSEC's support to CSIS is that it responds to requests for the release of Canadian identities that have been suppressed in foreign intelligence reporting. Upon receipt of a formal request, CSEC must be satisfied with the justification and lawful authority for requiring the information.

Findings

Overall, I am of the opinion that CSEC acted within its mandate in conducting activities in support of CSIS. I am in accord with the advice and guidance provided by the Department of Justice to CSEC respecting this support. However, in some cases, I question which part of CSEC's mandate should be used as the proper authority for conducting these activities and I have recommended that CSEC re-examine this matter. As of March 31, 2008, this was the subject of ongoing discussions between my officials and CSEC.

In addition, my office identified concerns respecting requests for the release of suppressed information, and respecting the CSIS-CSE Memorandum of Understanding of 1990 that guides the agencies' cooperation. Many of my findings reinforced those of two previous reviews of CSEC's foreign intelligence collection in support of the

RCMP and of the roles of CSEC's client relations officers and Operational Policy Section in the release of personal information, both of which are described in my 2006–2007 Annual Report.

I am pleased to note that since the period of review, CSEC continues to review its internal processes, policies and procedures, in order to make improvements in areas where deficiencies have been identified.

CSEC continues to make improvements in areas where deficiencies have been identified.

I have, however, recommended that CSEC re-visit the Memorandum of Understanding between CSIS and CSEC which is out of date and does not reflect current arrangements or practices between the two agencies. Given the international threat environment, it is my view that cooperation between security and intelligence agencies must be continually examined and the frameworks for cooperation kept up to date.

Reviews underway and planned

My office has several reviews underway that I will be reporting on to the Minister in the coming year and will include in my next Annual Report. The subjects of these reviews include: activities conducted by CSEC under several foreign intelligence ministerial authorizations; the disclosure of information about Canadians to federal government departments and agencies; an examination of certain common practices of CSEC related to its mandated activities, and a comprehensive study of its information technology security activities. Some reviews that will begin in the next fiscal year will carry through to 2009–2010. Last year I indicated that I would be reporting on CSEC's use of technology to protect the privacy of Canadians. At fiscal year-end, this review was being finalized, and therefore it will be reported on in next year's Annual Report.

Complaints about CSEC activities

My mandate includes undertaking any investigation I deem necessary in response to a complaint. During the 2007–2008 fiscal year my office received no complaints that warranted formal investigation.

Duties under the *Security of Information Act*

I have a duty under the *Security of Information Act* to receive information from persons who are permanently bound to secrecy and seek to defend the release of classified information about CSEC on the grounds that it is in the public interest. No such matters were reported to my office in the 2007–2008 fiscal year.

THE COMMISSIONER'S OFFICE

I continue to be supported in my work by a full-time staff of eight people, together with a number of subject matter experts who make themselves available, as required, under contract.

Keeping sufficiently current with technology to support my review of CSEC's activities is always a challenge. It was facilitated this year by CSEC itself. In the fall of 2007, CSEC opened its doors to members of my staff who attended two courses for CSEC employees, one respecting information technology security, and another course covering foreign intelligence.

In May 2007, I addressed a meeting of the Advisory Council on National Security that was held in Ottawa. The Advisory Council was created in April 2004 as a feature of the National Security Policy. It is made up of individuals from outside the government whose function is to provide advice on security matters.

Also in May, my office hosted a meeting of the Review Agencies Forum, which brings together the staff members of the Security Intelligence Review Committee, the Office of the Inspector General of the Canadian Security Intelligence Service, the Commission for Public Complaints against the Royal Canadian Mounted Police and my own office. The Forum provides an opportunity for review analysts to compare best practices and discuss issues of mutual interest and concern. In this regard, my office's review methodology initiative was discussed at length.

In June 2007, I had the pleasure of introducing U.S. Supreme Court Justice Antonin Scalia at the *International Conference on the Administration of Justice and National Security in Democracies*, held in Ottawa. The Conference, which was jointly sponsored by the Federal Court of Canada and the Canadian Centre of Intelligence and Security Studies at Carleton University, also provided me with an opportunity to renew my contacts with colleagues from other countries, some of whom I had met at the last *International Intelligence Review Agencies Conference* (*IIRAC*) in South Africa in October 2006.

Also in June, I was represented by the Executive Director at an international conference on Accountability of Intelligence and Security Agencies and Human Rights, held in The Hague under the auspices of the Dutch Review Committee on the Intelligence and Security Services and the Faculty of Law of Radboud University, Nijmegen. In September, I was represented by the Director of Operations at the annual conference of the Canadian Association for Security and Intelligence Studies in Calgary, where participants explored the many challenges facing the security and intelligence community.

Also in September, I attended a two-day conference entitled *Protecting Security and Human Rights: The Case for Migration in Canada* and sponsored by the Institute for Research in Public Policy.

All these initiatives demonstrate increasing interest, in Canada and abroad, in security and intelligence matters and their many dimensions.

Since its creation in 1996 by Order in Council pursuant to Part II of the *Inquiries Act*, the Office of the CSE Commissioner has been funded by the Department of National Defence, but has received administrative and other support from the Privy Council Office.

Over the fall months, a decision was taken that the long-standing relationship with the Privy Council Office would be severed, and that the administrative and other support activities for my office would be taken over by National Defence. I view this change in a positive light. I would be remiss, however, if I failed to take note of the outstanding help and support provided by the staff of the Privy Council Office over the last twelve years. Thank you from all of us.

In the interest of providing information about OCSEC's work, my office hosts a website (www.ocsec-bccst.gc.ca) that describes our mandate and activities. In fiscal year 2007–2008, there were over 98,000 visits to the site, including visitors from approximately 40 countries outside North America.

In 2007–2008, my office's expenditures were $1,220,999, which was well within budget for the period. Annex C to this report provides a summary of 2007–2008 expenditures.

A TRIBUTE

On November 24, 2007, the Right Honourable Antonio Lamer, my predecessor as CSE Commissioner, died at age 74. Antonio Lamer was a renowned lawyer and jurist. He was appointed to the Supreme Court of Canada in 1980, and was named Chief Justice in 1990, a position that he occupied until his retirement in 2000.

For my part, he was my colleague on the bench for over 11 years, and my long-standing friend. His contribution to Canadian jurisprudence was outstanding, exceeded only by his love of Canada. He is missed.

ANNEX A: MANDATE OF THE COMMUNICATIONS SECURITY ESTABLISHMENT COMMISSIONER

***National Defence Act* – Part V.1**

273.63 (1) The Governor in Council may appoint a supernumerary judge or a retired judge of a superior court as Commissioner of the Communications Security Establishment to hold office, during good behaviour, for a term of not more than five years.

(2) The duties of the Commissioner are

(a) to review the activities of the Establishment to ensure that they are in compliance with the law;

(b) in response to a complaint, to undertake any investigation that the Commissioner considers necessary; and

(c) to inform the Minister and the Attorney General of Canada of any activity of the Establishment that the Commissioner believes may not be in compliance with the law.

(3) The Commissioner shall, within 90 days after the end of each fiscal year, submit an annual report to the Minister on the Commissioner's activities and findings, and the Minister shall cause a copy of the report to be laid before each House of Parliament on any of the first 15 days on which that House is sitting after the Minister receives the report.

(4) In carrying out his or her duties, the Commissioner has all the powers of a commissioner under Part II of the *Inquiries Act*.

(5) The Commissioner may engage the services of such legal counsel, technical advisers and assistants as the Commissioner considers necessary for the proper performance of his or her duties and, with the approval of the Treasury Board, may fix and pay their remuneration and expenses.

(6) The Commissioner shall carry out such duties and functions as are assigned to the Commissioner by this Part or any other Act of Parliament, and may carry out or engage in such other related assignments or activities as may be authorized by the Governor in Council.

(7) The Commissioner of the Communications Security Establishment holding office immediately before the coming into force of this section shall continue in office for the remainder of the term for which he or she was appointed.

[...]

273.65 (8) The Commissioner of the Communications Security Establishment shall review activities carried out under an authorization issued under this section to ensure that they are authorized and report annually to the Minister on the review.

Security of Information Act

15. (1) No person is guilty of an offence under section 13 or 14 if the person establishes that he or she acted in the public interest. [...]

(5) A judge or court may decide whether the public interest in the disclosure outweighs the public interest in non-disclosure only if the person has complied with the following: [...]

(b) the person has, if he or she has not received a response from the deputy head or the Deputy Attorney General of Canada, as the case may be, within a reasonable time, brought his or her concern to, and provided all relevant information in the person's possession to, [...]

(ii) the Communications Security Establishment Commissioner, if the person's concern relates to an alleged offence that has been, is being or is about to be committed by a member of the Communications Security Establishment, in the purported performance of that person's duties and functions of service for, or on behalf of, the Communications Security Establishment, and he or she has not received a response from the Communications Security Establishment Commissioner within a reasonable time.

ANNEX B: CLASSIFIED REPORTS TO THE MINISTER, 1996–2008

1. Principal vs. agent status – March 3, 1997 (TOP SECRET)

2. Operational policies with lawfulness implications – February 6, 1998 (SECRET)

3. CSE's activities under *** – March 5, 1998 (TOP SECRET Codeword/CEO)

4. Internal investigations and complaints – March 10, 1998 (SECRET)

5. CSE's activities under *** – December 10, 1998 (TOP SECRET/CEO)

6. On controlling communications security (COMSEC) material – May 6, 1999 (TOP SECRET)

7. How we test (A classified report on the testing of CSE's signals intelligence collection and holding practices, and an assessment of the organization's efforts to safeguard the privacy of Canadians) – June 14, 1999 (TOP SECRET Codeword/CEO)

8. A study of the *** collection program – November 19, 1999 (TOP SECRET Codeword/CEO)

9. On *** – December 8, 1999 (TOP SECRET/COMINT)

10. A study of CSE's *** reporting process — an overview (Phase I) – December 8, 1999 (SECRET/CEO)

11. A study of selection and *** — an overview – May 10, 2000 (TOP SECRET/CEO)

12. CSE's operational support activities under *** — follow-up – May 10, 2000 (TOP SECRET/CEO)

13. Internal investigations and complaints — follow-up – May 10, 2000 (SECRET)

14. On findings of an external review of CSE's ITS program – June 15, 2000 (SECRET)

15. CSE's policy system review – September 13, 2000 (TOP SECRET/CEO)

16. A study of the *** reporting process — *** (Phase II) – April 6, 2001 (SECRET/CEO)

17. A study of the *** reporting process — *** (Phase III) – April 6, 2001 (SECRET/CEO)

18. CSE's participation *** – August 20, 2001 (TOP SECRET/CEO)

19. CSE's support to ***, as authorized by *** and code-named *** – August 20, 2001 (TOP SECRET/CEO)

20. A study of the formal agreements in place between CSE and various external parties in respect of CSE's Information Technology Security (ITS) – August 21, 2002 (SECRET)

21. CSE's support to ***, as authorized by *** and code-named *** – November 13, 2002 (TOP SECRET/CEO)

22. CSE's *** activities carried out under the *** 2002 *** Ministerial authorization – November 27, 2002 (TOP SECRET/CEO)

23. Lexicon of CSE definitions – March 26, 2003 (TOP SECRET)

24. CSE's activities pursuant to *** Ministerial authorizations including *** – May 20, 2003 (SECRET)

25. CSE's support to ***, as authorized by *** and code-named *** — Part I – November 6, 2003 (TOP SECRET/COMINT/CEO)

26. CSE's support to ***, as authorized by *** and code-named *** — Part II – March 15, 2004 (TOP SECRET/COMINT/CEO)

27. A review of CSE's activities conducted under *** Ministerial authorization – March 19, 2004 (SECRET/CEO)

28. Internal investigations and complaints — follow-up – March 25, 2004 (TOP SECRET/CEO)

29. A review of CSE's activities conducted under 2002 *** Ministerial authorization – April 19, 2004 (SECRET/CEO)

30. Review of CSE *** operations under Ministerial authorization – June 1, 2004 (TOP SECRET/COMINT)

31. CSE's support to *** – January 7, 2005 (TOP SECRET/COMINT/CEO)

32. External review of CSE's *** activities conducted under Ministerial authorization – February 28, 2005 (TOP SECRET/COMINT/CEO)

33. A study of the *** collection program – March 15, 2005 (TOP SECRET/COMINT/CEO)

34. Report on the activities of CSE's *** – June 22, 2005 (TOP SECRET)

35. Interim report on CSE's *** operations conducted under Ministerial authorization – March 2, 2006 (TOP SECRET/COMINT)

36. External review of CSE *** activities conducted under Ministerial authorization – March 29, 2006 (TOP SECRET/CEO)

37. Review of CSE's foreign intelligence collection in support of the RCMP (Phase II) – June 16, 2006 (TOP SECRET/COMINT/CEO)

38. Review of information technology security activities at a government department under ministerial authorization – December 18, 2006 (TOP SECRET)

39. Review of CSE signals intelligence collection activities conducted under ministerial authorizations (Phase I) – February 20, 2007 (TOP SECRET/COMINT/CEO)

40. Role of the CSE's client relations officers and the Operational Policy Section in the release of personal information – March 31, 2007 (TOP SECRET/COMINT/CEO)

41. Review of information technology security activities at a government department under ministerial authorization – July 20, 2007 (TOP SECRET)

42. Review of CSEC's counter-terrorism activities – October 16, 2007 (TOP SECRET/COMINT/CEO)

43. Review of CSE's activities carried out under a ministerial directive – January 9, 2008 (TOP SECRET/COMINT/CEO)

44. Review of CSEC's support to CSIS – January 16, 2008 (TOP SECRET/COMINT/CEO)

45. Review of CSEC signals intelligence collection activities conducted under ministerial authorizations (Phase II) – March 28, 2008 (TOP SECRET/COMINT/CEO)

ANNEX C: STATEMENT OF EXPENDITURES, 2007–2008

Standard Object Summary

Salaries and Wages	$713,135
Transportation and Telecommunications	37,431
Information	21,239
Professional and Special Services	257,488
Rentals	151,894
Purchased Repair and Maintenance	3,538
Materials and Supplies	8,652
Acquisition of Machinery and Equipment	23,258
Other Expenditures	4,364
Total	**$1,220,999**

ANNEX D: HISTORY OF THE OFFICE OF THE COMMUNICATIONS SECURITY ESTABLISHMENT COMMISSIONER (OCSEC)

The Office of the Communications Security Establishment Commissioner (OCSEC) was created on June 19, 1996, with the appointment of the inaugural Commissioner, the Honourable Claude Bisson, O.C., a former Chief Justice of Québec, who held the position until June 2003. He was succeeded by the Right Honourable Antonio Lamer, P.C., C.C., C.D., LL.D., D.U., Chief Justice of Canada (retired) for a term of three years. The Honourable Charles D. Gonthier, C.C., Q.C., who retired as Justice of the Supreme Court of Canada in 2003, was appointed as Commissioner in August 2006.

For the first six years (from June 1996 to December 2001), the Commissioner carried out his duties under the authority of Orders in Council issued pursuant to Part II of the *Inquiries Act*. During this period, the Commissioner's responsibilities were twofold: to review the activities of the Communications Security Establishment Canada (CSEC) to determine whether they conformed with the laws of Canada; and to receive complaints about CSEC's activities.

Following the terrorist attacks in the United States on September 11, 2001, Parliament adopted the omnibus *Anti-terrorism Act* which came into force on December 24, 2001. The omnibus *Act* introduced amendments to the *National Defence Act*, by adding Part V.1 and creating legislative frameworks for both OCSEC and CSEC. It also gave the Commissioner new responsibilities to review activities carried out by CSEC under a ministerial authorization.

The omnibus legislation also introduced the *Security of Information Act*, which replaced the *Official Secrets Act*. This legislation gives the Commissioner specific duties in the event that a person, who would otherwise be permanently bound to secrecy, seeks to defend the release of classified information about CSEC on the grounds that it is in the public interest.

Under the Commissioner's current mandate, which entrenched in law the original mandate established in 1996 as well as the additional responsibilities described above, the Commissioner has retained the powers of a commissioner under Part II of the *Inquiries Act*.

ANNEX E: ROLE AND MANDATE OF THE COMMUNICATIONS SECURITY ESTABLISHMENT CANADA (CSEC)

The Communications Security Establishment Canada (CSEC) is Canada's national cryptologic agency. Unique within Canada's security and intelligence community, CSEC employs code-makers and code-breakers to provide the Government of Canada with information technology security and foreign intelligence services. CSEC also provides technical and operational assistance to federal law enforcement and security agencies.

CSEC's foreign intelligence products and services support government decision-making in the fields of national security, national intelligence and foreign policy. CSEC's signals intelligence activities relate exclusively to foreign intelligence and are directed by the Government of Canada's intelligence priorities.

CSEC's information technology security products and services enable its clients (other government departments and agencies) to effectively secure their electronic information systems and networks. CSEC also conducts research and development on behalf of the Government of Canada in fields related to communications security.

CSEC has a three-part mandate under subsection 273.64(1) of the *National Defence Act*. These are known as parts (a) (b) and (c) of its mandate:

(a) to acquire and use information from the global information infrastructure for the purpose of providing foreign intelligence, in accordance with Government of Canada intelligence priorities;

(b) to provide advice, guidance and services to help ensure the protection of electronic information and of information infrastructures of importance to the Government of Canada; and

(c) to provide technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties.